

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

BCRS1 LLC,

Plaintiff,

v.

MAREK LASKOWSKI and KARL CAMOTA,

Defendants.

Civil Action No.

COMPLAINT

Plaintiff BCRS1 LLC (“BCRS1”), by its undersigned counsel, for its amended complaint against defendants, alleges as follows:

JURISDICTION AND VENUE

1. This civil action arises under Section 1030 *et seq.* of the Computer Fraud and Abuse Act (“CFAA,” or the “Act”), 18 U.S.C. § 1030 *et seq.*; jurisdiction is founded on the existence of questions pleaded herein under the Act.

2. As detailed below, defendants unlawfully accessed one or more protected computers and damaged plaintiff in excess of \$5,000 during a one-year period. Therefore, this action may be brought pursuant to the CFAA, 18 U.S.C. § 1030(g) and 18 U.S.C. § 1030(c)(4)(A)(i)(I).

3. Venue is proper in this District pursuant to 27 U.S.C. §1391(b), in that it is a judicial district in which plaintiff is domiciled and in which defendants caused the damages by unlawfully accessing and damaging plaintiff’s protected computers.

4. This Court has supplemental jurisdiction of plaintiff’s various state law claims pursuant to 28 U.S.C. Section 1367(a).

PARTIES

5. Plaintiff is a limited liability company duly organized and existing under the laws of the State of New Jersey and is domiciled in New Jersey

6. Defendant Marek Laskowski is a natural person, and a citizen of Ontario, Canada.

7. Defendant Karl Camota is a natural person, and a citizen of Ontario, Canada.

BACKGROUND

A. Plaintiff's Agreement With Novera

8. Plaintiff is engaged in the business of providing technical computer services to over the counter cryptocurrency traders.

9. The domain name "CHOMPBTC" is owned by plaintiff, BCRS1 LLC.

10. At all relevant times to this complaint, BCRS2 LLC was a company with common ownership with plaintiff.

11. BCRS2 LLC has no ownership interest in Plaintiff's Protected Server or Plaintiff's Website Technology as hereinafter defined.

12. To the extent that defendant claims that BCRS2 LLC possesses any claim or interest concerning the subject matter of this action, BCRS2 LLC has previously assigned such interest and claims to plaintiff.

13. Plaintiff maintains the web server, website and associated computer software and technology for the "CHOMPBTC" domain.

14. In or about February 2020, plaintiff entered into an agreement (the "Consulting Agreement") with Novera Capital Inc. ("Novera") through its CEO Jacob Unger.

15. The Agreement provided that Novera would develop a computer program which would include an electronic trading platform for *inter alia* “Over the Counter” cryptocurrency traders (the “Web Site Platform”).

16. The Agreement provided for Novera to develop the Web Site Platform for plaintiff pursuant to the specifications to be provided by plaintiff.

17. The Web Site Platform was intended to be licensed to plaintiff’s customers and generate revenue for plaintiff and its customers.

18. The Web Site Platform was to provide an easy-to-purchase platform for the purchase of cryptocurrencies.

19. The Web Site Platform was also required to record all transactions and provide backend accounting services.

20. The Web Site Platform was to be developed exclusively for plaintiff.

21. Plaintiff retained ownership of all code, computer software, trade secrets and information used for the Web Site Platform (collectively “Plaintiff’s Website Technology”).

22. The Web Site Platform was to be developed and stored on plaintiff’s protected computer server (“Plaintiff’s Protected Server”).

23. Unger represented to plaintiff that the cost of the Web Site Platform would be reimbursement for the wages of the software developers employed by Novera of approximately \$25,000 per month.

24. Unger represented to plaintiff that the Web Site Platform would be completed within three months by June 2020.

25. Unger represented that at that time Novera had no other customer projects and that Novera would dedicate practically all of its resources to timely develop the Web Site Platform.

26. Unger also represented that at that time Novera had no other sales and income and that plaintiff's payments were needed by Novera for its payroll.

27. Plaintiff remitted in excess of \$85,000 to Novera.

28. Plaintiff performed all of its obligations pursuant to the Agreement.

29. Novera provided a beta version of the Web Site Platform.

30. Novera failed to deliver the final Web Site Platform pursuant to the terms of the Agreement.

B. Unger's and Defendants' Scheme With Novera

i. Unger Schemes For a \$1 Million Investment

31. In 2018, Unger founded Novera. (Unger Dep. 12:13.)¹

32. Unger testified that Novera was based on an idea "to create a protocol for decentralized assets and decentralized finance." (Unger Dep. 30:5-9.)

33. Unger testified that Novera is a "syntec" company that was in the business of developing blockchain technology for use in cryptocurrency. (Unger Dep. 9: 6-10.)

34. Unger testified that Novera attempted "to create a new type of financial technology that would be very useful to a lot of people in the crypto space and the traditional financial world. That was going to be powered by blockchain and mostly decentralized blockchain." (Unger Dep. 31:13-18.)

¹ Unger Dep. refers to the sworn deposition of Jacob Unger conducted on January 12, 2022 in an action entitled BCRS1 LLC v. Unger, 20-cv-04246 (E.D.N.Y).

35. Unger testified that he received funding from venture capitalists. (Unger Dep. 12:13-19.)

36. Upon information and belief, Unger received in excess of \$1 million from the venture capitalists (the “\$1 Million VC Investment”).

37. Upon information and belief, Unger was a scam artist who regularly used Novera’s funds and income to pay his personal expenses and commingled his expenses with Novera’s expenses.

38. Upon information and belief, Unger transferred part of the \$1 Million VC Investment funds and other of Novera’s funds to himself and others on his behalf.

39. Unger testified that Novera never produced any viable technology product. (Unger Dep. 31:21-25, 32:1-7.)

40. Unger testified that other than plaintiff and an affiliated entity, Novera did not have any customers for any technology product. (Unger Dep. 33:3-5, 35:10-13.)

41. In reality, Novera was not a real technology company, but was a shell with a few employees and with no real assets, which Unger used to fleece investors.

42. Upon information and belief, Unger never accounted for the \$1 Million VC Investment.

ii. Unger and Defendants Scheme Plaintiff For An Additional Investment

43. Approximately one year after receiving the \$1 Million VC Investment, Unger began seeking a new victim for his scam.

44. In or about 2019, Unger began courting plaintiff’s principal, David Eisenberger (“Eisenberger”), to obtain funds from Eisenberger.

45. Unger represented to Eisenberger that he could assist him with the financial books and setup for one of Eisenberger's affiliated entities, JVerify.

46. Unger testified that Novera's first consulting job was in 2019, when its Chief Financial Officer assisted in setting up the JVerify's "books." (Unger Dep. 36:4-11.)

47. In 2019 and 2020, Unger continued to court Eisenberger and claimed that Novera was a technology company with valuable technology patents and ability to create new technology.

48. Unger testified that the deal between him and plaintiff was that "Novera would provide employees and contractors at cost for a short term consulting. . . engagement to some particular issues" without paying any sort of overhead. (Unger Dep. 43:17-25.)

49. Unger represented to plaintiff that the Web Site Platform would be complete in or about June 2020.

50. Unger testified that the agreement with plaintiff was open ended, and the agreement would expire when "A, Novera ran out of the money or, B, Novera had a new investor or new investor structure where something that could change our corporate structure at which point this deal would no longer be approved by Novera. So it was -- I wouldn't say that it was open-ended, but it was impossible to put a timeline or something that we didn't know exactly what was going to happen." (Unger Dep. 53:2-10)

51. Based on Unger's representations, in or about March 2020, plaintiff entered into the Consulting Agreement with Novera.

52. Contrary to Unger's representation in 2019 and 2020 that he had the means to develop the Web Site Platform for plaintiff, Unger testified that, at the time that the consulting

agreement commenced, Novera did not possess technology useful for plaintiff. (Unger Dep. 37:16-21.)

53. Unger recently testified that in 2020, Novera began consulting with plaintiff because plaintiff was having issues with its bookkeeping and accounting concerning plaintiff's existing technology. (Unger Dep. 36:12-17.)

54. Unger recently testified that the purpose of the Consulting Agreement was to make plaintiff's existing technologies of bookkeeping and accounting more feasible. (Unger Dep. 37:8-15.)

55. Unger recently testified that plaintiff already possessed a product and that Novera's consulting was only going to develop a "tool" to apply to plaintiff's product. (Unger Dep. 37:22-25, 38-1-3.)

56. Unger testified that "Novera provided consulting work, mostly revolving around the issue of creating some sort of tooling or infrastructure searches that would be helpful to BCRS in their accounting, compliance and bookkeeping needs." (Unger Dep. 43:2-16.)

57. Unger's testimony was materially different than his representations to plaintiff in 2019 and 2020.

58. From March through May 2020, Unger continued to represent to plaintiff that Novera was an advanced technology company.

59. From March through June 8, 2020, plaintiff worked with Novera's employees, including software engineers defendants Marek Laskowski and Karl Camota.

60. Unger testified that plaintiff provided direction of the services through Unger and that Unger then directed defendants Laskowski and Camota and others to provide the services. (Unger Dep. 47:13-19.)

61. During this period, Laskowski and Camota worked on Plaintiff's Website Technology.

62. Pursuant to the Consulting Agreement, plaintiff paid the wages for defendants Laskowski, Camota and other Novera employees.

63. Unger testified that plaintiff paid "the salaries to Mr. Camota, Mr. Herrera, Mr. Laskowski and Ms. Tullo for the work that they did at the rate they were paid," i.e., the cost without any profit or overhead. (Unger Dep. 46:6-15.)

64. Pursuant to the Consulting Agreement, plaintiff did not pay any overhead nor any profit margin to Novera.

65. From March through June 8, 2020, Unger continued to represent to plaintiff's principal that Novera was an advanced company with very valuable technology patents.

66. From March through June 8, 2020, Unger continued to represent to plaintiff's principal that Novera only required approximately \$300,000 to be able to bring Novera's patented technology to market.

67. Unger convinced plaintiff's principal through BCRS Ventures LLC to invest approximately \$300,000 into Novera (the "BCRS Ventures Investment").

68. On or about June 8, 2020, BCRS Ventures LLC and Novera entered into the BCRS Ventures Investment.

iii. Unger's Scheme To Extort Plaintiff and Defendant's Hacking

69. Immediately after the BCRS Ventures Investment, Unger began to extort plaintiff for additional funds, plaintiff's technology assets and future revenue.

70. At that time, Unger disputed the terms of the Consulting Agreement and claimed that he should receive additional compensation from plaintiff.

71. Although Novera was required to complete the Web Site Platform, Unger stated that Novera would not complete the final version of the Web Site Platform unless plaintiff agreed to relinquish ownership of its Plaintiff's Website Technology and provide for him to share in plaintiff's revenues.

72. Unger testified that the consulting agreement ended on June 8, 2020, when BCRS Ventures LLC purchased an interest in Novera. (Unger Dep. 56:24-25, 57:1-2, 59:9-11.)

73. When pressed for the terms of the Consulting Agreement, Unger recently testified that he is "a little bit fuzzy on" the agreement and "a bit vague because it was a verbal agreement." (Unger Dep. 55:20-23.)

74. Unger testified that on or prior to June 8, 2020, he directed all of Novera's staff, including defendants, not to perform any computer work for plaintiff with "the exception of a consulting for a transition plan." (Unger Dep. 59:17-22.)

75. Unger testified that in June 2020, defendants Camota and Laskowski and other Novera employees, stopped doing any work for plaintiff or any entity with common ownership to plaintiff. (Unger Dep. 63:13-18.)

76. Unger testified that all consulting work for plaintiff ceased between June 8, 2020, and June 15, 2020. (Unger Dep. 60:22-25, 61:1-10, 62:17-20, 100:5-16.)

77. In June through August 2020, Unger attempted to extort plaintiff's future revenue and Plaintiff's Website Technology from plaintiff.

78. Plaintiff would not agree to Unger's extortion, agree to pay any additional funds, relinquish any ownership to Plaintiff's Website Technology, nor relinquish any future revenue.

79. Unger became angrier and claimed that he could not understand why plaintiff would not agree to relinquish any ownership to Plaintiff's Website Technology nor future revenue.

80. In an effort to pressure plaintiff, Unger declared Novera insolvent. (Unger Dep. 73:16-18.)

81. On August 25, 2020, Unger transmitted via text an acknowledgment that plaintiff owned Plaintiff's Website Technology. (Unger Dep. 174:19-21.)

82. At that time, Unger claimed that Plaintiff's Website Technology would be worthless without Unger. (Unger Dep. 174:19-21.)

83. Unger refused to allow any Novera employees to complete the Web Site Platform and perform any consulting services for plaintiff. (Unger Dep. 60:22-25, 61:1-10, 62:17-20, 100:5-16.)

84. At that time, Unger threatened plaintiff that the cost to replace Plaintiff's Website Technology would be at least \$200,000 and would require plaintiff to remake Plaintiff's Website Technology. (Unger Dep. 174:22-25, 175:1-19.)

85. Despite Unger's threats, plaintiff refused to pay any additional funds, relinquish any ownership to Plaintiff's Website Technology or agree to split future revenue.

86. Unbeknownst to plaintiff, on August 25, 2020, while Unger was threatening plaintiff and attempting to extort plaintiff, defendants accessed Plaintiff's Protected Server, copied Plaintiff's Website Technology and also disabled plaintiff's Web Site Platform.

87. Defendants accessed Plaintiff's Protected Server despite Unger having represented to plaintiff that defendants and others would not perform any consulting services on Plaintiff's Protected Server.

88. Defendants accessed Plaintiff's Protected Server despite having been directed by Unger not to perform any consulting services on Plaintiff's Protected Server since June 8, 2020.

89. Without plaintiff's authorization, on Aug 25, 2020, at 11:16am through 11:28am, defendants accessed Plaintiff's Protected Server, copied Plaintiff's Website Technology and did the following:

- (i) created project "Novera / otc-core;"
- (ii) copied "new branch master" at Novera / otc-core;
- (iii) pushed new branch feature/web3-integration at Novera / otc-core;
- (iv) created project Novera / otc-trading;
- (v) pushed new branch master at Novera / otc-trading;
- (vi) pushed new branch demo at Novera / otc-trading;
- (vii) created project Novera / otc-admin;
- (viii) pushed new branch master at Novera / otc-admin; and
- (ix) pushed to branch feature/web3-integrationat Novera / otc-core.

90. Two days after accessing Plaintiff's Protected Server and copying Plaintiff's Website Technology, on August 27, 2020, Unger emailed a threat to reveal confidential information obtained from Plaintiff's Protected Server:

You had told me that you don't want a revenue split . . . Do you really want to shine a light on any of the BCRS entities? Even if you feel that you have done nothing wrong and that you would win in court, you would have to open up a lot of information that I know you would not be comfortable with

91. Plaintiff would not accede to Unger's extortion.

92. Plaintiff did not agree to share its revenues, its Web Site Platform and Plaintiff's Website Technology.

93. Defendants knew that plaintiff was relying on the Web Site Platform and Plaintiff's Website Technology to continue its businesses.

94. Only five days after Unger's latest threat, on or about September 2, 2020, defendants accessed Plaintiff's Protected Server. (Unger Dep. 133:17-18.)

95. On or about September 2, 2020, Comota accessed Plaintiff's Protected Server and copied all of Plaintiff's Website Technology to Novera's Github Account.

96. On September 2, 2020, between 4:06pm and 5:24pm, defendants accessed Plaintiff's Protected Server without authorization and deleted the following computer files and folders which were part of Plaintiff's Website Technology:

- (i) branch feature/gemini-withdrawal at ChompBTC / ChompCore API;
- (ii) branch bug-fix-trading at ChompBTC / ChompCore API;
- (iii) branch feature/withdrawal-requests at ChompBTC / ChompCore API;
- (iv) branch feature/chomp-clearing at ChompBTC / ChompCore API;
- (v) branch release-1.3at ChompBTC / ChompCore API;
- (vi) branch dev at ChompBTC / ChompCore API;
- (vii) branch b at ChompBTC / ChompCore API; and
- (viii) branch rollback at ChompBTC / ChompCore API.

97. On September 2, 2020, as a result of defendants' unlawfully accessing Plaintiff's Protected Server, Plaintiff's Web Site Platform became inoperable.

98. On September 2, 2020, Unger, and defendants Camota and Laskowski, sent emails to each other which state in pertinent part:

Hi All,

I just completed the source code rollback on GitLab [Plaintiff's Server] and uploaded the latest copy to the Novera Github Account.

I also reverted the deployed binaries on Chomp's Sandbox environment [Plaintiff's Website], this probably broke the current sandbox app [Plaintiff's Website].

Regards,
Karl

99. The email response from Laskowski to Camota asked Unger:

Jacob - is there anything else you wanted Karl you do with respect to Chomp? [Plaintiff's Website]

100. Unger responded in pertinent part:

Thank you, Karl.

101. Thereafter, plaintiff demanded that Unger and Novera return the Plaintiff's Website Technology, but Unger and Novera refused.

102. As a result of defendants' actions, plaintiff was required to rebuild Plaintiff's Website Platform.

FIRST CLAIM FOR RELIEF
Violation of Computer Fraud and Abuse Act "(CFAA)"
And Conspiracy to Violate the CFAA
18 USC 1030(a)(2)(c); (a)(5)(A); (a)(5)(B); (a)(5)(B); (a)(7)(B); (a)(7)(B); (b); and (g)

103. Plaintiff repeats and realleges each of the allegations set forth in the paragraphs above as if fully set forth herein.

104. Plaintiff is the sole owner of Plaintiff's Protected Server.

105. Plaintiff was in control of Plaintiff's Protected Server.

106. Plaintiff is the sole owner of Plaintiff's Website Technology.

107. Plaintiff was in control of Plaintiff's Website Technology.

108. Plaintiff is the sole owner of the Web Site Platform.

109. Plaintiff was in control of the Web Site Platform.

110. Plaintiff's Website Technology included the Web Site Platform, together with the associated programming code, structure, and trade secrets.

111. As set forth above, Unger claims that the consulting agreement between Novera and plaintiff terminated prior to June 15, 2020.

112. As set forth above, from June 8, 2020, through August 2020, Unger repeatedly advised plaintiff's principal and all of Novera's employees that they should not provide any computer services to plaintiff.

113. At the time, Unger advised plaintiff that Novera would not provide any additional services for plaintiff.

114. Defendants were not authorized to access Plaintiff's Protected Server on and after August 25, 2020.

115. Defendants were not authorized to copy Plaintiff's Website Technology to Novera's account and for Novera's use.

116. Defendants were not authorized to disable Plaintiff's Website Technology.

117. From on or about August 25, 2020, through September 2, 2020, after the relationship between plaintiff and Novera had terminated, defendants accessed Plaintiff's Protected Server and Plaintiff's Website Technology.

118. Plaintiff's Website Technology including the Web Site Platform, the code repository, logins, passwords, and other confidential information are, and were known by defendants to be confidential information and knowledge.

119. As set forth above, defendants deleted computer files and folders which were part of Plaintiff's Website Technology.

120. As set forth above, defendants caused Plaintiff's Website Technology to be unusable.

121. As a direct result of defendants' accessing Plaintiff's Protected Server and deleting part of Plaintiff's Website Technology, plaintiff was unable to use Plaintiff's Website Technology.

122. By email on dated Wednesday, September 2, 2020, at 4:49PM, defendant Camota advised defendant Laskowski and Unger that he removed Plaintiff's Website Technology from Plaintiff's Protected Server and placed Plaintiff's Website Technology into Novera's "Github Account."

123. Defendant Camota also acknowledged to Unger and defendant Laskowski that his actions "probably" destroyed Plaintiff's Website Technology including the Web Site Platform.

124. Unger and defendant Laskowski acknowledged receipt of defendant Camota's email in which defendant Camota admitted that he accessed Plaintiff's Protected Server.

125. Defendants' conduct affected protected computers used in and affecting interstate and foreign commerce.

126. Defendant Camota is a foreign individual, residing in Ontario, Canada, who unlawfully accessed Plaintiff's Protected Server in the United States.

127. Defendant Laskowski is a foreign individual, residing in Ontario Canada who unlawfully accessed Plaintiff's Protected Server in the United States.

128. Unger and defendants knew that their conduct affected protected computers used in and affecting interstate and foreign commerce.

129. Defendants knowingly, maliciously, and unlawfully engaged in unlawful access of Plaintiff's Protected Server.

130. Defendants obtained Plaintiff's Website Technology by unlawfully accessing Plaintiff's Protected Server in violation of CFAA, 18 USC 1030(a)(2)(c).

131. Defendants knowingly transmitted a program, information, code, or command, to or through Plaintiff's Protected Server, and as a result of such conduct, intentionally caused damage to Plaintiff's Website Technology in violation of CFAA, 18 USC 1030(a)(5)(A).

132. Defendants intentionally and without authorization accessed Plaintiff's Protected Server and as a result of such conduct, recklessly caused damage to plaintiff in violation of CFAA, 18 USC 1030(a)(5)(B).

133. Defendants intentionally and without authorization accessed Plaintiff's Protected Server and as a result of such conduct, recklessly caused damage to plaintiff in violation of CFAA, 18 USC 1030(a)(5)(C).

134. As detailed above, defendants, with intent to extort from plaintiff money and other things of value, transmitted in interstate or foreign commerce communications containing threats to cause damage to Plaintiff's Protected Server in violation of CFAA, 18 USC 1030(a)(7)(A).

135. Defendants, with intent to extort from plaintiff money and other things of value, transmitted in interstate or foreign commerce a threat to obtain information from Plaintiff's Protected Server without authorization or in excess of authorization and to impair the confidentiality of information obtained from Plaintiff's Protected Server without authorization or by exceeding authorized access in violation of CFAA, 18 USC 1030(a)(7)(B).

136. Defendants with intent to extort from plaintiff money and other things of value, transmitted in interstate or foreign commerce a demand for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion in violation of CFAA, 18 USC 1030(a)(7)(B).

137. Defendants conspired with Unger and others to commit the CFAA violations as described above in violation of CFAA, 18 USC 1030(b).

138. As a result of the defendants' actions, plaintiff was required to rebuild its website and server, and to date, has been damaged in excess of \$200,000.

139. Plaintiff has been damaged by defendants' unlawful and malicious conduct in an amount in excess of \$5,000 during a one-year period.

SECOND CLAIM FOR RELIEF
Tortious Interference With Contracts and
Tortious Interference With Prospective Economic Advantage

140. Plaintiff repeats and realleges each of the allegations set forth above, as if fully set forth herein.

141. As detailed above, defendants intentionally and unlawfully accessed Plaintiff's Protected Server and other protected computers.

142. As detailed above, defendants intentionally and unlawfully accessed Plaintiff's Protected Server, including without limitation, defendants (i) copied Plaintiff's Website Technology; (ii) deleted part of Plaintiff's Website Technology; and (iii) rendered plaintiff's Web Site Platform unusable.

143. Plaintiff was creating a website for its customers to use to buy and sell cryptocurrency.

144. Defendants were aware of plaintiff's business.

145. Defendants engaged in unlawfully accessing Plaintiff's Protected Server in order to interfere with plaintiff's potential business relations.

146. Defendants interfered with plaintiff's opportunities of creating and running the Web Site Platform and providing services to potential customers.

147. Defendants acted with the sole purpose of harming plaintiff.

148. Defendants' conduct was unlawful and/or used wrongful means.

149. As a result of the forgoing conduct by defendants, upon information and belief, plaintiff was damaged and continues to be damaged in excess of \$500,000, the exact amount to be determined at trial.

150. Defendants' conduct was malicious and shocking to the conscience. Therefore, defendant should also be held liable for punitive damages to prevent him, and others similarly inclined from repeating such tortuous conduct in the future, in the sum of at least \$500,000, the precise amount to be determined at trial.

THIRD CLAIM FOR RELIEF
Prima Facie Tort

151. Plaintiff repeats and realleges each of the allegations set forth in above, as if fully set forth herein.

152. As detailed above, defendants intentionally and unlawfully accessed Plaintiff's Protected Server and other protected computers.

153. As detailed above, defendants intentionally accessed Plaintiff's Protected Server, including without limitation, defendant (i) copied Plaintiff's Website Technology; (ii)

deleted part of Plaintiff's Website Technology; and (iii) rendered plaintiff's Web Site Platform unusable.

154. Upon information and belief, defendants claim that they were authorized to access the Plaintiff's Protected Server and that their actions were lawful.

155. To the extent that defendants' conduct was lawful in whole or in part, defendants used such means to harm plaintiff.

156. Defendants' conduct was performed with the intention of inflicting harm on plaintiff and its business.

157. Defendants' conduct was without any excuse or justification.

158. Defendants' conduct resulted in special damages.

159. As a result of the foregoing conduct by defendants, upon information and belief, plaintiff was damaged and continues to be damaged in excess of \$500,000, the exact amount to be determined at trial.

160. Defendants' conduct was malicious and shocking to the conscience. Therefore, defendants should also be held liable for punitive damages to prevent him, and others similarly inclined from repeating such tortuous conduct in the future, in the sum of at least \$500,000 the precise amount to be determined at trial.

FOURTH CLAIM FOR RELIEF **Negligence**

161. Plaintiff repeats and realleges each of the allegations set forth in paragraphs 1-86 above, as if fully set forth herein.

162. As detailed above, defendants, directly or indirectly, intentionally and unlawfully accessed Plaintiff's Protected Server other protected computers.

163. Defendants, directly or indirectly, accessed Plaintiff's Protected Server, and negligently damaged Plaintiff's Website Technology when defendants (i) copied Plaintiff's Website Technology; (ii) deleted part of Plaintiff's Website Technology; and (iii) rendered plaintiff's Web Site Platform unusable.

164. Defendants' conduct was with the intention of inflicting harm on plaintiff and its business.

165. Defendants' conduct was without any excuse or justification.

166. Defendants' conduct was unlawful.

167. As a result of the forgoing conduct by defendant, upon information and belief, plaintiff was damaged and continues to be damaged in excess of \$500,000, the exact amount to be determined at trial.

168. Defendants' conduct was malicious, shocking to the conscience. Therefore, defendant should also be held liable for punitive damages to prevent him, and others similarly inclined from repeating such tortuous conduct in the future, in the sum of at least \$500,000 the precise amount to be determined at trial.

RELIEF REQUESTED

WHEREFORE, plaintiff demands judgment in its favor and against defendant as follows:

A. awarding compensatory damages in an amount in excess of \$500,000, the precise amount to be determined at trial;

B. awarding punitive damages in an amount in excess of \$500,000;

C. preliminarily and permanently:

- i. compelling defendant to return to plaintiff all confidential or proprietary information and all property that is in his possession and which belongs to plaintiff;
- ii. enjoining defendant from taking any further actions to interfere with plaintiff and plaintiff's property;

D. awarding plaintiff its costs and disbursements of this action, including attorney's fees;

and

E. awarding plaintiff such other and further relief as this court may deem just and proper.

Plaintiff demands a jury on all issues so triable.

Dated: March 11, 2022
New York, New York

LAW OFFICE OF JEFFREY FLEISCHMANN PC
By: /s/Jeffrey Fleischmann
Jeffrey Fleischmann, Esq.

Attorneys for Plaintiff

150 Broadway, Suite 900
New York, N.Y. 10038
Tel. (646) 657-9623
Fax (646) 351-0694
jf@lawjf.com